IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

United States of America

v. Docket No. 7:22-CR-1

Jerald Francis Gray

Defendant's Motion to Suppress Evidence

This case presents the following question: does a Magistrate act as a rubber stamp when he grants a search warrant based on an affidavit that merely describes aspects of a method police claim to use to uncover criminal activity without actually telling the judge the method police used? In other words, if counsel described general principles of baking and then averred that counsel used those methods to produce bread, could the court make its own determination about the quality of counsel's bread? Or about the veracity of counsel's claims? No. The court, to the extent that it would make its own opinion about whether counsel produced bread, should be given the recipe—the metaphorical item (the algorithm) not given to the magistrate in this case.

Brief factual summary

The internet is awash in images of child sexual abuse. Though many social media and web-based companies have recently taken measures to curb their role in this market, many parts of the internet value privacy over surveillance. Freenet is an internet-based program that people can use to share files with one another, to receive files, and to encrypt and store files. Many aspects of Freenet shield the identity of its users, allowing people to share files without easily identifying themselves. In short, to hide the identity of its users, Freenet makes it difficult for someone to know whether a person using the program is merely using the program passively or whether that person is downloading specific files. Freenet hides its users activity by making it appear as though all its users are engaging in very similar conduct. However, each person who uses Freenet to share files necessarily identifies himself through his IP address. Unless a person using Freenet has also taken steps to anonymize one's IP address, it is possible to track a person's activity to his or her identity.

Freenet essentially works by connecting individual users to other users of the network. Users do not connect to every other user of Freenet, but to a small subset of users each time the user starts the program. A user might receive a software key that will allow the user to download a file that has been encrypted and stored in small parts among various other users of the Freenet program. To download the file, a person enters the key and begins sending requests to the user's peers. If a peer has portions of the file, it returns those to the requestor. It may then resend the request to its peer users, and so on. The software limits the number of times a request may be referred to others (Hops-to-live, or HTL value)—preventing the program from continuously requesting files ad infinitum. Users can set the number of times they wish to have the requests sent to another's peers—this number is not controlled by the Freenet program.

Law Enforcement has investigated Freenet because of its capacity to allow users to share images of child sexual abuse. The government worked with a professor at the University of Massachusetts at Amherst to develop an algorithm that it believes it can use to positively identify whether a Freenet user is the original requestor of a file or whether the user is simply forwarding another's request. In turn, if law enforcement has identified the file as one involving child sexual abuse images, it could reliably know if a person was requesting such material. However, the algorithm appears farcical. The government instead seems simply to count the number of remaining HTL. If the HTL value is 17 or 18, and if the number of file bits requested is roughly similar to the quotient of the total file bits and the requestor's peer-network, the government claims that algorithm has determined that such a requestor is in fact the originator of the request and, thus, a device from which someone attempted to download prohibited material.

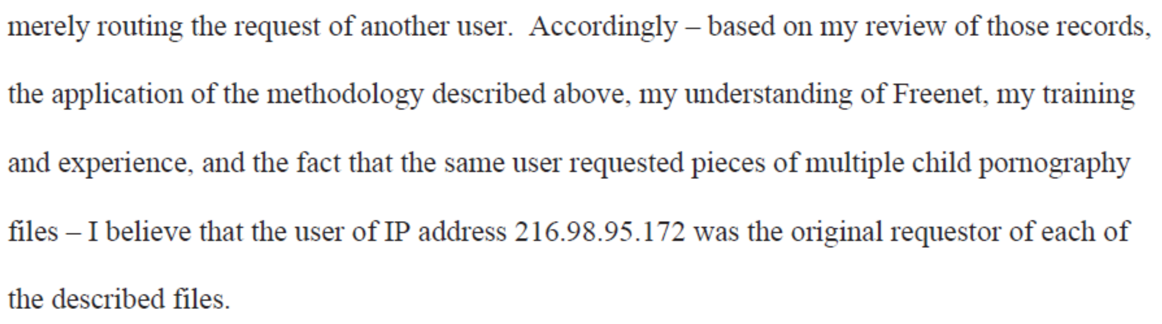
Investigators filed a thirty-six page affidavit in support of their request to search Mr. Gray's home for his computer, hard drives, and other electronic storage media. The affidavit extensively described Freenet, how the program generally works, and how one could look at aspects of code to help to discover whether a user was the requestor of a file or merely a user sending along another's request. However, the affidavit did not include the algorithm the government claimed to use.

Indeed, only about a page of that affidavit referenced investigative techniques actually employed in this case. And none of the information contained on that page enabled the Magistrate to make an independent finding of whether the government established probable cause. Instead, the government simply requested that the Magistrate trust that it used a secret method alluded to, but not disclosed, and that the method accurately identified Mr. Gray's computer as a requestor of child sexual abuse images.

Argument

"Warrant affidavit[s] must set forth particular facts and circumstances underlying the existence of probable cause, so as to allow the magistrate to make an independent evaluation of the matter." *See Franks v. Delaware*, 438 U.S. 154, 165 (1978). Importantly, the magistrate's "action cannot be a mere ratification of the bare conclusions of others" and must be based on "sufficient information . . . to determine probable cause . . ." *See United States v. Leon*, 468 U.S. 897, 915 (1984) (quoting *Illinois v. Gates*, 462 U.S. 213, 239 (1983)). Magistrates cannot serve as a "rubber stamp for the police." *Leon*, at 914.

At its heart, the warrant requirement ensures that probable cause determinations are not made by police, but by a neutral and detached judicial officer with sufficient information to assess the credibility of the police claims. *See United States v. Harris*, 403 U.S. 573, 590 (1971). In this case, though, police failed to tell the court how it was that they determined that Mr. Gray's computer was the originator of a request for a known image of contraband. Indeed, each time law enforcement describes finding evidence that Mr. Gray's computer accessed contraband, their conclusions are hedged by reference to myriad items not reviewable by the magistrate, which include: the actual methodology and algorithm police used; how that algorithm was actually applied in this case; and the law enforcement officer's understanding of Freenet and training and experience. The affidavit makes this plain as day:



> merely routing the request of another user. Accordingly – based on my review of those records, the application of the methodology described above, my understanding of Freenet, my training and experience, and the fact that the same user requested pieces of multiple child pornography files – I believe that the user of IP address 216.98.95.172 was the original requestor of each of the described files.

Without providing the magistrate with an understandable description of the algorithm used in this case and a description of how it in fact was used in this case, the magistrate was not given enough information to allow him to adequately assess whether the police were acting on probable cause. As such, the magistrate acted as a rubber stamp.

Additionally, police knew that they were intentionally withholding the algorithm from the court and withholding key information necessary for the Magistrate to conduct an independent assessment of probable cause. No reasonable officer should knowingly rely on an affidavit issued by a magistrate when the magistrate was not given the key information necessary for the magistrate to assess probable cause. Exclusion is appropriate.

Respectfully submitted

Benjamin Schiffelbein
Assistant Federal Public Defender
210 First Street SW, Ste 400
Roanoke, VA 24011
Benjamin_Schiffelbein@fd.org